Cost-effective Secure E-health Cloud System Using Identity Based Cryptographic Techniques

Xu An Wang[1,3], Jianfeng Ma[2], Fatos Xhafa[4], Mingwu Zhang[5], Xiaoshuang Luo[3]

[1]*School of Telecommunications Engineering, Xidian University, P. R. China*
[2]*School of Cyber Engineering, Xidian University, P. R. China*
[3]*Engineering University of Chinese Armed Police Force, P. R. China*
[4]*Department of Computer Science, Technical University of Catalonia, Spain*
[5]*Hubei University of Technology, P. R. China*
wangxazjd@163.com

Abstract

Nowadays E-health cloud systems are more and more widely employed. However the security of these systems needs more consideration due to the sensitive health information of patients. So far, some protocols about secure e-health cloud systems have been proposed, but many of them use the traditional PKI infrastructure to implement cryptographic mechanisms, which is cumbersome as they require every user having and remembering its own public/private keys. Identity based encryption (IBE) is a cryptographic primitive, which uses the identity information of the user (e.g., email address) as the public key. Hence, the public key is implicitly authenticated and the certificate management is greatly simplified. On the other hand, proxy re-encryption is a cryptographic primitive aiming at transforming a ciphertext under the delegator A's into another ciphertext, which can be decrypted by the delegatee B. In this paper, we describe several identity related cryptographic techniques for securing an E-health system, which include new IBE schemes and new identity based proxy re-encryption (IBPRE) schemes. We also prove these schemes' security and give their performance analysis. Our results show that our IBPRE scheme is especially highly efficient for re-encryption, which can be used to achieve cost-effective cloud usage.

Keywords: Secure e-health cloud system, identity based encryption, identity based proxy re-encryption, cost-effective.

1. Introduction

E-health System. E-health systems nowadays are becoming more and more commonplace in medical systems by integrating information technology and traditional medical diagnosis processes [23]. Traditionally, when a person has some health troubles, he/she goes to the hospital to see a doctor. The doctor needs to carefully check patient's body state to decide the potential kind of disease or health trouble. In this process, the doctor may need to handle images, referrals, medical records, etc. which is usually a tedious task.

E-health systems can help handling this work automatically, by means of the health care information system. For instance, in China, as one typical application of the promising *Internet+* technology, it is expected that in the near future, E-health will be one of the most practical public administration services. In particular, the Electronic Health Records (EHR) plays a central role in any E-health system; they can be recorded by doctors and nursers, collected by sensors in wireless body sensor network, etc. By using an E-health system, doctors can freely share and exchange health records, while patients can easily access to their health records through a designated patient's portal, and the health care providers can enquire patients' time-critical and general data effectively and transparently. Additionally, E-health systems can be beneficial to other users and stakeholders in the field. Thus, the system stores the patient's medical history and is a vital information source for physicians. We can see an overview on a typical E-health system in Fig. 1. Clinicians record EHRs and related events summary from E-health system consumers and longitudinal health records. These EHRs can be further supplied to hospitals and other medical providers for deep analysis like lab tests. Health IT vendors can also better support the hospitals from these health records by dynamically adjusting their policy. Administers, funders or researchers can also benefit from this process. However, all these benefits come to the risk of unauthorized data access, data sharing or data leakage, among other unauthorized patient's data usage. Indeed, security and privacy are one of the main issues that prevent to widely adapt E-health systems, for electronic health records are sensitive information. Malicious attackers can use them to endanger the patient's life. Although there are proposals on how to secure the E-health system, many of them use traditional PKI infrastructure to implement cryptographic mechanisms and this is not convenient nor practical for many users. In this paper, we show how to secure E-health systems, mainly using fuzzy biometric E-health system using the identity based cryptographic techniques, without requiring certificates from the end-user.

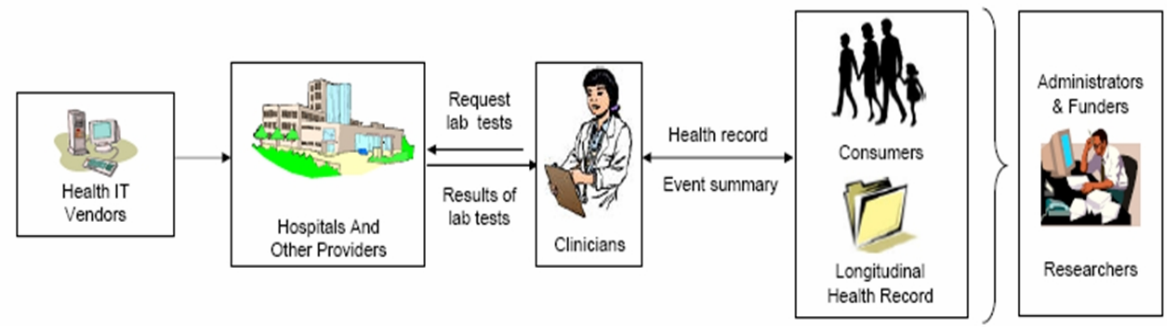

Figure 1: Overview of an E-health System.

IBE scheme. In 1984, Shamir [41] introduced the concept of identity-based cryptography to ease the certificate management in traditional public key system. A user's public key in an IBE scheme is the identity information of the user (e.g., email address). Hence the public key is implicitly authenticated and the certificate management is greatly simplified.

However, the first practical IBE scheme [8] was only proposed 17 years after its concept was proposed. Since then, many practical IBE schemes with different properties have been proposed [9, 40, 44, 18].

Until now, there are many interesting applications of IBE, but there is almost no work on how to apply them to the E-health system. Although we can see some work on using attribute based encryption (ABE) in the E-health system, but still there is no work concentrating on how to handle identities directly in these systems. If we can directly use some string such as the email address as the identity public key, then the workload of patients can be decreased significantly. We can see an overview on IBE in Fig. 2. In Fig. 2, Alice encrypted her health information using identity "bob@medical.com" to doctor Bob, while doctor Bob requests his private key from the CA/PKG.

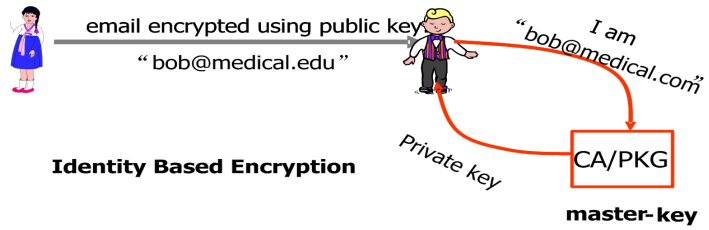

Figure 2: Overview on IBE scheme.

IBPRE scheme. The concept of proxy re-encryption (PRE) is proposed by Blaze *et al.* [7] in 1998, which allows a semi-trusted proxy, with some information (a.k.a., the re-encryption key), to translate a ciphertext under the delegator's public key into another ciphertext, which can be decrypted by the delegatee's secret key. However, the proxy cannot access the plaintext. According to the direction of transformation, PRE schemes can be classified into bidirectional and unidirectional schemes. Also, according to the times the transformation can apply to the ciphertext, PRE schemes can be classified into single-hop and multi-hop schemes. At NDSS'05, Ateniese *et al.* [1] proposed a few unidirectional PRE schemes and discussed its several potential applications such as distributed secure file systems. Later, many unidirectional PRE schemes with different properties have been proposed [24, 50, 43, 38, 14, 49]. Due to the simpler certificate management in IBE, Green and Ateniese [17] extended PRE to the IBE setting, i.e. identity based proxy re-encryption (IBPRE). They also discussed its several interesting applications such as bridging IBE and PKE. Since then, several IBPRE schemes have been proposed [13, 31, 43, 37, 14, 51], but none of them, except [38, 14], can achieve master secret secure: the corrupted proxy and delegatee cannot derive the delegator's private key. However, IBPRE schemes in [38] are generic constructions relying on CCA-secure 2-level hierarchical ID-based (2,2) threshold cryptosystem but they are inefficient. IBPRE schemes in [14] rely on conditional proxy broadcast re-encryption; they are also inefficient and can only achieve secure against replayable chosen ciphertext attacks (RCCA). We can see an overview on IBPRE in Fig. 3. In Fig. 3, a patient encrypts his/her health information using doctor's identity "Doctor@medical.com" , and outsources the ciphertexts to the cloud. In the setup phase, the

Doctor has sent the re-encryption key to the proxy, and thus the proxy can re-encrypt the ciphertexts to be the ciphertexts under the assistant doctor's identity "AssistantDoctor@medical.com" . By using IBPRE, the assistant doctor shares the patient's health information without the cloud knowing about any sensitive information.

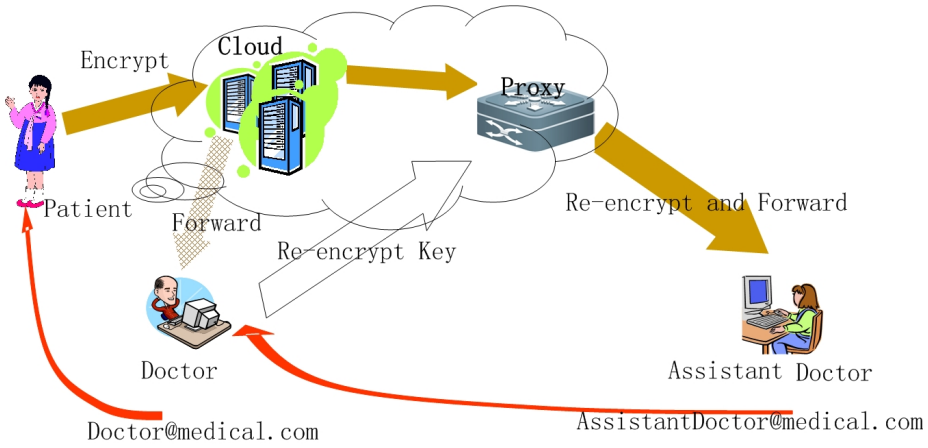

Figure 3: Overview on IBPRE

1.1. Our Contribution

In this paper, we show how to securely integrate the IBE and IBPRE schemes into an E-health cloud system, and thus exploring on how to use identity related cryptographic techniques for securing an E-health cloud system, especially on the confidential property. We also propose novel IBE and IBPRE schemes and prove their security. Although there exist many IBE schemes with different properties, however one part of the private key in all these IBE schemes is of the form: $y = f(msk)$, where msk is the master key and y is an element in the underlying bilinear group $\mathbb{G}$. We construct a new identity based encryption scheme. The main novelty of our IBE is that: one part of the private key is $y = f(msk)$, where msk is the master key and y is an element in $\mathbb{Z}_p^*$. Here, p is the underlying bilinear group's prime order. To resist the adversary to extract useful information on the master key from this part of the private key, we introduce some randomness in the private key. We prove this new IBE is IND-sID-CPA secure in the standard model based on a related DBDH assumption in the bilinear groups. Furthermore, we propose an IBPRE scheme on this new IBE scheme. This new IBPRE scheme does not follow Green's paradigm on which almost all the existing efficient IBPRE schemes are based. The main novelty in this IBPRE is that, the re-encryption key is almost independent with the delegatee's private key. As a result, our IBPRE can achieve *master secret security*. Finally, we analyse the security of the proposed E-health cloud system and also show the performance of our IBPRE scheme, which is the critical part of the whole system. Indeed, our IBPRE scheme has a unique feature which almost no other IBPRE schemes have, that is, it is very efficient for re-encryption. Considering that re-encryption is the most often operation cloud systems implement for secure E-health system, and that this operation must be paid by data users

or data owners, our IBPRE scheme can be high cost-effective for E-health cloud system users.

1.2. Related Work

Cryptographic Techniques for Securing E-health systems. Until now there are published several proposals on how to use cryptographic techniques for securing E-health systems, including using symmetric key and public key schemes, or pseudo anonymous ID technique, etc. A common belief on the security of E-health system is that the EHRs should be encrypted to protect security and privacy. Data, identifiers (pseudonyms), keys and data attributes (meta-data) are all needed to be encrypted before storing them on the central authority or outsourcing them to the cloud. Although the centralized facility or the employees of the cloud service providers are assumed to be prohibited from obtaining the information about the encrypted PHR, but that assumption could go into detriment of the whole system's usability. How to establish the access control properly and to handle the key management problem effectively is of critical importance. Cryptographic techniques can also be used to enforce the secure access control mechanism or the key management properly [27, 28, 20, 33, 34]. Here, we discuss some results closely related to our proposals. Benaloh *et al.* [6] discussed how to use encryption for electronic medical records to ensure privacy by a new paradigm called patient controlled encryption. Li *et al.* [25, 26] discussed how to implement the fine-grained data access control in multi-owner settings of patient-centric PHRs by using attribute based encryption (ABE). Barua *et al.* [5] also proposed a framework called ESPAC to handle the access control problem by using ABE. Guo *et al.* [19] proposed a privacy-preserving attribute-based authentication system for eHealth networks. Aleman *et al.* [3] reviewed carefully the literature on EHRs and discussed the current research state on security and privacy on E-health systems.

IBE scheme. Here we start by recalling the IBE and FIBE schemes closely related to our work. At Crypto'01, Boneh and Franklin constructed the first practical identity based encryption based on bilinear groups [8] (BF IBE). In 2003, Sakai and Kasahara proposed a new identity based encryption with different structure based on bilinear groups (SK IBE) [40]. However, both of these works proved their security in the random oracle model. At Eurocrypt'04, Boneh and Boyen proposed two new efficient selective identity secure IBE schemes without random oracles (BB_1 IBE and BB_2 IBE) [9]. Later Boneh and Boyen [10], Waters [44] improved their work on IBE schemes with full security at Crypto'04 and Eurocrypt'05 (Waters' IBE). At Eurocrypt'06, Gentry proposed an efficient identity based encryption with tight security proof in the standard model but based on a strong assumption (Gentry's IBE) [18]. All the existing IBEs are based on three frameworks: "Full Domain Hash" framework, " Exponent Inversion" framework and "Communicative Blinding" framework [11]. "Full Domain Hash" framework includes BF IBE, which is proven secure in the random oracle and supports hierarchies and threshold variants. "Exponent Inversion" framework includes SK IBE, BB_2 IBE and Gentry's IBE, which are always difficult to support extensions. "Communicative Blinding" framework includes BB_1 IBE and Waters' IBE, which always support extensions like hierarchy IBE, threshold IBE, fuzzy IBE, attribute based encryption and broadcast encryption.

IBPRE scheme. In ACNS'07, Green and Ateniese proposed the first identity based proxy re-encryption schemes [17]. They defined the algorithms and security models for identity based proxy re-encryption, and constructed their scheme by using a variant of the efficient Dodis/Ivan key splitting approach to settings with a bilinear map. The re-encryption key in their scheme is of the form $(\mathsf{H}_1(\mathsf{Alice})^{-s} \cdot \mathsf{H}(\mathsf{X}), \mathsf{IBE}_{Bob}(\mathsf{X}))$. When the proxy re-encrypts, it does some transformations and sends $\mathsf{IBE}_{Bob}(\mathsf{X})$ to the delegatee. And then, the delegatee decrypts $\mathsf{IBE}_{Bob}(\mathsf{X})$ to recover X and uses this X to recover the original message. In ISC'07, Chu and Tzeng proposed the first IND-CCA2 secure proxy re-encryption in the standard model based on Waters' IBE [13]. They followed the paradigm proposed in [17] (denoted here it as Green's paradigm). Unfortunately, Shao *et al.* found their scheme cannot achieve IND-CCA2 secure and they fixed this flaw by proposing an improved scheme [39]. However, both of these schemes are not efficient due to the structure of Waters' IBE and Green's paradigm. In Pairing'07, Matsuo proposed four types of proxy re-encryption: IBE to IBE, CBE to IBE, IBE to CBE and CBE to CBE. They constructed a hybrid proxy re-encryption scheme from CBE to IBE and a proxy re-encryption scheme from IBE to IBE. But recently it was shown that their proxy re-encryption scheme from IBE to IBE has some flaws [46]. In Inscrypt'08, Tang *et al.* proposed the new concept of inter-domain identity based proxy re-encryption [43]. They were concerned on constructing proxy re-encryption between different domains in identity based setting. They follow Green's paradigm but based on Boneh-Frankin IBE. Their scheme can only achieve IND-sID-CPA secure. Later, Ibraimi *et al.* construct a type and identity based proxy re-encryption, which aimed at combing type and identity properties in one proxy re-encryption system [21]. Recently, Lai *et al.* [29] gave new constructions on IBPRE based on identity-based mediated encryption. Luo *et al.* [30] also gave a new generic IBPRE construction based on IBE. Wang *et al.* proposed the first multi-use CCA-secure unidirectional IBPRE scheme [45]. Until now, although there are some proposals on how to achieve attribute based proxy re-encryption, but there is almost no work on how to achieve fuzzy IBPRE scheme.

1.3. Paper's Organization

In Section 2, we give some preliminaries, including the assumptions, definitions and security models. In Section 3, we present the overview on our E-health system model, propose our schemes and analyse their security. In Section 5, we give the performance analysis on our proposed IBPRE scheme, which is a critical part of our E-health system. Finally, we conclude our paper in the last Section 6.

2. Preliminaries

2.1. Bilinear Groups

Let $\mathcal{G}$ be an algorithm called a group generator that takes as input a security parameter λ and outputs a tuple (G, G_T, e) where $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups of order p, and e is a function $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ satisfying the following properties:

- (Bilinear) $\forall u, v \in \mathbb{G}, \forall a, b \in Z$,

$$e(u^a, v^b) = e(u, v)^{ab}$$

- (Non-degenerate) $\exists g \in \mathbb{G}$ such that $e(g, g)$ has order p in $\mathbb{G}_T$.

We assume that the group action in $\mathbb{G}$ and $\mathbb{G}_T$ as well as the bilinear map e are all computable in polynomial time in λ. Furthermore, we assume that the description of $\mathbb{G}$ and $\mathbb{G}_T$ includes a generator of $\mathbb{G}$ and $\mathbb{G}_T$ respectively.

2.2. EXDBDH1 Assumption

EXDBDH1 assumption extends the DBDH assumption in the prime order bilinear group.

Definition 1. *Run $\mathcal{G}$ to obtain $(\mathbb{G}, \mathbb{G}_T, e)$. Next it generates g as generators of $\mathbb{G}$. On input $(g, g^a, g^b, g^c,$
$g^{(b+c)d}, g^d, T)$, for any probabilistic polynomial time algorithm $\mathcal{A}$ cannot distinguish $T = e(g, g)^{abd}$ from a random element in $\mathbb{G}$ with non-negligible probability, this is the EXDBDH2 assumption.*

We note that the assumption is a falsifiable assumption [32]. Intuitively, there is no g^{ab}, g^{ad}, g^{bd}, hence the pairing cannot help to solve the decisional problem.

2.3. Definition and Security Notion for IBE

An IBE scheme consists of the following algorithms.

Setup(1^k). On input a security parameter, outputs both the master public parameters params which are distributed to users, and the master key msk which is kept private.

KeyGen$(msk,$ params, $ID)$. On input an identity $ID \in \{0,1\}^*$ and the master secret key msk, outputs a decryption key sk_{ID} corresponding to that identity.

Encrypt$(ID,$ params, $m)$. On input a set of public parameters, an identity $ID \in \{0,1\}^*$ and a plaintext $m \in M$, outputs C_{ID}, the encryption of m under the specified identity.

Decrypt$(sk_{ID},$ params, $C_{ID})$. Decrypts the ciphertext C_{ID} using the secret key sk_{ID}, and outputs m or $\perp$.

We recall the IND-sID-CPA security in [9]. It is defined using the following game:

Init: The adversary outputs an identity ID^* where it wishes to be challenged.

Setup: The challenger runs the Setup algorithm. It gives the adversary the resulting system parameters params. It keeps the master key to itself.

Phase1: The adversary issues $q_1 \cdots q_m$ where q_i is one of private key query ID_i where $ID_i \neq ID^*$. The challenger responds by running algorithm KeyGen to generate the private key d_i corresponding to the public key ID_i. It sends d_i to the adversary. These queries maybe asked adaptively, that is, each query q_i may depend on the replies to $q_1, \cdots, q_{i-1}$.

Challenge: Once the adversary decides that Phase1 is over it outputs two equal length plaintexts $M_0, M_1 \in \mathsf{M}$ on which it wishes to be challenged. The challenger picks a random bit $b \in \{0,1\}$ and sets the challenge ciphertext to $\mathsf{C} = \mathsf{Encryption}(\mathsf{params}, \mathsf{ID}^*, \mathsf{M}_b)$. It sends C as the challenge to the adversary.

Phase2: The adversary issues additional queries $q_{m+1} \cdots q_n$ where q_i is one of private key queries ID_i where $ID_i \neq ID^*$. The challenger responds as in Phase1. These queries maybe asked adaptively as in Phase1.

Guess: Finally, the adversary outputs a guess $b' \in \{0,1\}$. The adversary wins if $b = b'$.

We refer to such an adversary $\mathcal{A}$ as an IND-sID-CPA adversary. We define the advantage of the adversary $\mathcal{A}$ in attacking the scheme $\mathcal{E}$ as $Adv_{\epsilon,Aa} =\mid Pr[b = b'] - \frac{1}{2} \mid$, The probability is over the random bits used by the challenger and the adversary. If this probability is negligible, then we say scheme $\mathcal{E}$ is IND-sID-CPA secure.

2.4. Definition and Security Notion for IBPRE

An identity based (single-hop) proxy re-encryption scheme consists of the algorithms **(Setup, KeyGen, Encrypt, Decrypt, ReKeygen, Reencrypt):**

Setup(1^k). On input a security parameter, outputs both the master public parameters params, which are distributed to users, and the master key msk which is kept private.

KeyGen(params, msk, ID). On input an identity $ID \in \{0,1\}^*$ and the master secret key msk, outputs a decryption key sk_{ID} corresponding to that identity.

Encrypt(params, ID, m). On input a set of public parameters, an identity $ID \in \{0,1\}^*$ and a plaintext $m \in M$, outputs the second level ciphertext C_{ID}, which can be re-encrypted by the proxy.

ReKeygen(params, sk_{ID_1}, ID_2). On input secret key sk_{ID_1}, and identities $ID_2 \in \{0,1\}^*$, the delegator non-interactively generates the re-encryption key $rk_{ID_1 \to ID_2}$ and outputs it.

Reencrypt(params, $rk_{ID_1 \to ID_2}$, C_{ID_1}). On input a second level ciphertext C_{ID_1} under identity ID_1, and a re-encryption key $rk_{ID_1 \to ID_2}$, outputs a first level re-encrypted ciphertext C_{ID_2} which can not be re-encrypted.

Decrypt$_2$(params, sk_{ID}, C_{ID}). On input a second level ciphertext C_{ID} under identity ID with secret key sk_{ID}, decrypts the ciphertext C_{ID}, and outputs m or $\perp$.

Decrypt$_1$(params, sk_{ID}, C_{ID}). On input a first level re-encrypted ciphertext C_{ID} under identity ID with secret key sk_{ID}, decrypts the re-encrypted ciphertext C_{ID}, and outputs m or $\perp$.

Correctness: Intuitively, an IBPRE is correct if the Decrypt algorithm always outputs the expected decryption of a properly generated ciphertext. Slightly more formally, let $c_{ID_1} \leftarrow Encrypt(params, ID_1, m)$ be a properly generated ciphertext, Then $\forall m \in \mathcal{M}, \forall ID_1, ID_2 \in \{0,1\}^*$, where $sk_{ID_1} = KeyGen(msk, ID_1)$, $sk_{ID_2} = KeyGen(msk, ID_2)$, $rk_{ID_1 \to ID_2} \leftarrow ReKeygen(params, sk_{ID_1}, ID_1, ID_2)$, the following propositions hold:

- Decrypt(params, sk_{ID_1}, c_{ID_1})= m
- Decrypt(params, sk_{ID_2}, Reencrypt(params, $rk_{ID_1 \to ID_2}$, c_{ID_1}))=m

IND-ID-CCA Security for the Second Level Ciphertext.. IND-ID-CCA Security for the second level ciphertext is defined according to the following game.

Setup. Run Setup(1^k) to get (params, msk), and give params to $\mathcal{A}$.

Find phase. $\mathcal{A}$ makes the following queries. At the conclusion of this phase $\mathcal{A}$ will select $ID^* \in \{0,1\}^*$ and $(m_0, m_1) \in \mathcal{M}^2$.

1. For $\mathcal{A}$'s queries to extract oracle $O_{extract}$ with $(extract, ID)$, return sk_{ID} =KeyGen(params, msk, ID) to $\mathcal{A}$.
2. For $\mathcal{A}$'s queries to re-encryption key extract oracle $O_{rkextract}$ with $(rkextract, ID_1, ID_2)$, where $ID_1 \neq ID_2$, return $rk_{ID_1 \to ID_2}$=ReKeygen(params, KeyGen(params, msk, ID_1), ID_2) to $\mathcal{A}$.
3. For $\mathcal{A}$'s queries to re-encrypt oracle $O_{reencrypt}$ with $(reencrypt, ID_1, ID_2, C)$, derive a re-encryption key $rk_{ID_1 \to ID_2}$ = ReKeygen(params, KeyGen(params, msk, ID_1), ID_2), and return C'=Reencrypt(params, $rk_{ID_1 \to ID_2}$, ID_1, ID_2, C) to $\mathcal{A}$.
4. For $\mathcal{A}$'s queries to the first level ciphertext decrypt oracle $O_{1decrypt}$ with $(decrypt, ID, C)$ where C is a first level ciphertext, return m = Decrypt$_1$(params, KeyGen(params, msk, ID), C) to $\mathcal{A}$.

Note that $\mathcal{A}$ is not permitted to choose ID^* such that trivial decryption is possible using keys extracted during this phase (e.g., by using extracted re-encryption keys to translate from ID^* to some identity for which $\mathcal{A}$ holds a decryption key). Also note that the second level ciphertext decrypt oracle $O_{2decrypt}$ is no use here, for any second level ciphertext can be first re-encrypted and then be queried to the $O_{1decrypt}$ to get the decryption result.

Choice and Challenge. When $\mathcal{A}$ presents $(choice, ID^*, m_0, m_1)$, choose $i \leftarrow_R \{0,1\}$, compute C^*= Encrypt(params, ID^*, m_i) and give C^* to $\mathcal{A}$.

Guess stage. $\mathcal{A}$ continues to make queries as in the find stage, with the following restrictions. Let $\mathcal{C} = (C^*, ID^*)$. For all rk given to $\mathcal{A}$, let $\mathcal{C}'$ be the set of all possible values

derived via calls to Reencrypt oracle, e.g. on successful execution of re-encrypt query $(reencrypt, ID^*, ID', C^*)$, let C' be the result and add the pair (C', ID') to the set $\mathcal{C}'$. We call $\mathcal{C} \cup \mathcal{C}')$ is the Derivative of (C^*, ID^*).

1. $\mathcal{A}$ is not permitted to issue any query of the form $(decrypt, ID, C)$ to decrypt oracle $O_{1decrypt}$ or $O_{2decrypt}$ where $(C, ID) \in (\mathcal{C} \cap \mathcal{C}')$.
2. $\mathcal{A}$ is not permitted to issue any queries $(ex-tract, ID)$ to extract oracle $O_{extract}$ or $(rk - extract, ID_1, ID_2)$ to re-encryption key extract oracle $O_{rkextract}$ that would permit trivial decryption of any ciphertext in (C, C').
3. $\mathcal{A}$ is not permitted to issue any query of the form $(reencrypt, ID_1, ID_2, C)$ to re-encrypt oracle $O_{reencrypt}$ where $\mathcal{A}$ possesses the keys to trivially decrypt ciphertexts under ID_2 and $(C, ID_1) \in (\mathcal{C} \cap \mathcal{C}')$.

At the conclusion of this stage, $\mathcal{A}$ outputs i', where $i' \in \{0, 1\}$.

The outcome of the game is determined as follows: If $i' = i$ then $\mathcal{A}$ wins the game. Let $Adv = \mid Pr(i' = i) - 1/2 \mid$. If for all probabilistic polynomial time algorithms $\mathcal{A}$, $Adv \leq v(k)$, we say that the IBPRE scheme $\mathcal{S}$ is IND-ID-CCA secure for the second level ciphertext.

IND-ID-CCA Security for the First Level Ciphertext.. IND-ID-CCA Security for the first level ciphertext is defined according to the following game.

Setup. Run Setup(1^k) to get (params, msk), and give params to $\mathcal{A}$.

Find phase. $\mathcal{A}$ makes the following queries. At the conclusion of this phase $\mathcal{A}$ will select $(ID^\star, ID^*) \in \{0, 1\}^*$ and $(m_0, m_1) \in \mathcal{M}^2$.

1. For $\mathcal{A}$'s queries to extract oracle $O_{extract}$ with $(extract, ID)$, return sk_{ID} =KeyGen (params, msk, ID) to $\mathcal{A}$.
2. For $\mathcal{A}$'s queries to re-encryption key extract oracle $O_{rkextract}$ with $(rkextract, ID_1, ID_2)$, where $ID_1 \neq ID_2$, return $rk_{ID_1 \to ID_2}$=ReKeygen(params, KeyGen(params, msk, ID_1), ID_2) to $\mathcal{A}$.
3. For $\mathcal{A}$'s queries to the first level ciphertext decrypt oracle $O_{1decrypt}$ with $(decrypt, ID, C)$, return m = Decrypt$_1$(params, KeyGen(params, msk, ID), C) to $\mathcal{A}$.

Note here that $\mathcal{A}$ is permitted to get all the extracted re-encryption keys including ID^* to some identity for which $\mathcal{A}$ holds a decryption key. Also note here that the re-encrypt oracle and second level ciphertext decrypt oracle are useless, since the $\mathcal{A}$ knows all the re-encryption key, he can do all the re-encryption and transform the second level ciphertext to the first level ciphertext.

Choice and Challenge. When $\mathcal{A}$ presents $(choice, ID^\star, ID^*, m_0, m_1)$, choose $i \leftarrow_R \{0, 1\}$, compute $C^\star$= Encrypt(params, ID^*, m_i) and C^*=Reencrypt(params, $rk_{ID^* \to ID^\star}$, $ID^\star$, ID^*, $C^\star$) give $C^\star$ to $\mathcal{A}$.

Guess stage. $\mathcal{A}$ continues to make queries as in the find stage, with the following restrictions.

1. $\mathcal{A}$ is not permitted to issue any query of the form $(decrypt, ID^*, C^*)$ to decrypt oracle $O_{1decrypt}$ or $(decrypt, ID^\star, C^\star)$ to $O_{2decrypt}$. Note here that $C^\star$ maybe can be derived from C^*.
2. $\mathcal{A}$ is not permitted to issue any queries $(extract, ID^\star)$ or $(extract, ID^*)$ to extract oracle $O_{extract}$.

At the conclusion of this stage, $\mathcal{A}$ outputs i', where $i' \in \{0, 1\}$.

The outcome of the game is determined as follows: If $i' = i$ then $\mathcal{A}$ wins the game. Let $Adv = \mid Pr(i' = i) - 1/2 \mid$. If for all probabilistic polynomial time algorithms $\mathcal{A}$, $Adv \leq v(k)$, we say that the IBPRE scheme $\mathcal{S}$ is IND-ID-CCA secure for the first level ciphertext.

Remark 1. *In this security notion, we give two target identities $(ID^*, ID^\star)$ for our re-encryption not randomizing the second level ciphertext. From the the re-encrypted first level ciphertext, anyone can trivially derive its second level ciphertext.*

Master Secret Security.. We extend Libert and Vergnaud's definition on master secret security of PRE [24], to IBPRE. This notion demands that no coalition of dishonest delegatees be able to pool their re-encryption keys in order to expose the private key of their common delegator. More formally, the following probability should be negligible as a function of the security parameter λ[1],

$$\begin{aligned} Pr[sk_{ID^\star} \leftarrow O_{extract}(ID^\star), \\ sk_{ID_x} \leftarrow O_{extract}(ID_x)\}, \\ \{R_{ID^\star \to ID_x} \leftarrow O_{rkextract}(ID^\star, ID_x)\}, \\ \{R_{ID_x \to ID^\star} \leftarrow O_{rkextract}(ID_x, ID^\star)\}, \\ \gamma \leftarrow \mathcal{A}(ID^\star, \{ID_x, sk_{ID_x}\}, \\ \{R_{ID^\star \to ID_x}\}, \{R_{ID_x \to ID^\star}\}) : \gamma = sk_{ID^\star}] \end{aligned}$$

3. System Model

Here we overview the proposed system model in Fig. 4. In this system model, there are four parties playing different roles: the patients, the physician group, the community health service group and the cloud. We can roughly describe the system as the following:

[1]Notations: ($ID^\star$, $sk_{ID^\star}$) denotes the target user's identity and private key and (ID_x, sk_{ID_x}) denotes the colluding user's identity and private key.

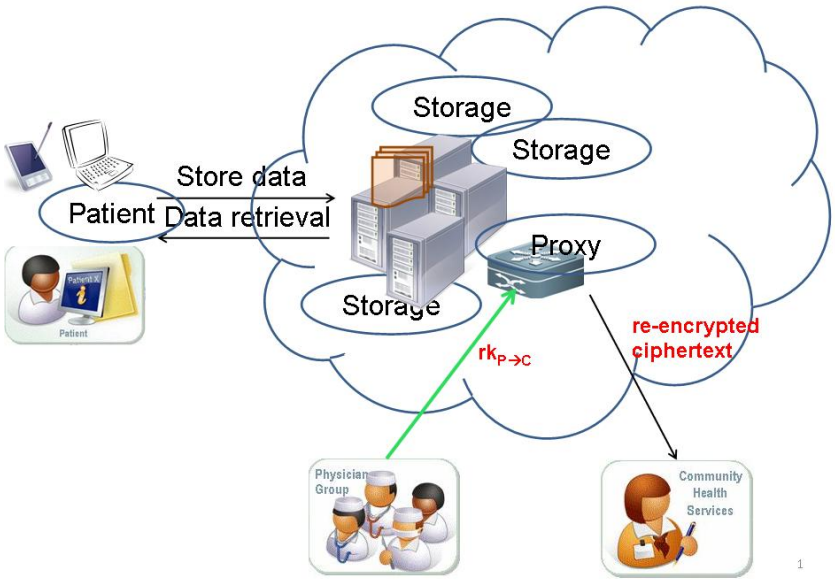

Figure 4: Our Proposed System Model

1. The system first setup the parameters and generate the public/secret keys for different parties. Here, the whole system runs in an identity based setting. All the users in the system including the patients, the physician group, the community health service group, all need to publish their identities as the public key, and they will obtain their secret keys corresponding to their identities via the IBE's Key Generation algorithm.
2. The patients or the physician group or the community health service group, first encrypt the EHRs using block ciphers like AES using block cipher key, then they encrypt the block cipher key using the target receivers' identities as the public keys (including their own identities), via the IBE's Encrypt algorithm, finally they outsource the ciphertexts corresponding to the EHRs or the keys to the cloud.
3. The patients, the physician group and the community health service group can retrieve the related ciphertexts from the cloud, and then recover the block cipher key from the ciphertexts via the IBE's Decrypt algorithm, finally they can recover the EHRs by using AES's decryption algorithm.
4. Suppose one day a patient Alice has been given a diagnosis by the physician group $\mathcal{R}$, and she encrypted her own EHRs under the physician group $\mathcal{R}$'s identities. But after that, some day when she is at home, she has a health trouble and wants the community health service group $\mathcal{T}$ can give her some assistance. If the community health service group $\mathcal{T}$ can have Alice's old EHRs, then this will greatly reduce their workload on the new diagnosis.
5. For easily obtaining Alice's old EHRs, the physician group $\mathcal{R}$ and the community health service group $\mathcal{T}$ have better to establish a proxy re-encryption mechanism

between them. Considering the setting in our system model, it is better to have an IBPRE mechanism. To smoothly run this mechanism, $\mathcal{R}$ need first generate the re-encryption key by using its own private key and $\mathcal{T}$'s identities, via running the ReKeyGen algorithm of IBPRE. Then $\mathcal{R}$ sends it to the proxy which is a semi-honest party which could be the cloud itself.

6. After obtaining the re-encryption requirement of the community health service group $\mathcal{T}$, the proxy (or the cloud) can implement the re-encryption and forward the re-encrypted ciphertexts to the community health service group $\mathcal{T}$. $\mathcal{T}$ then uses its own secret key to decrypt the re-encrypted ciphertext to obtain the patient $\mathcal{T}$'s EHRs.

Here we describe the security objectives of our E-health system model.

1. For the patients, the physician group, and the community health service group, their encrypted EHRs need to be kept confidential for the adversary, thus the ciphertexts should achieve IND-ID-CPA or IND-ID-CCA security, that is, the ciphertexts should be indistinguishable for the adversary under chosen plaintext attack or chosen ciphertext attack.
2. For the physician group, which runs the proxy re-encryption mechanism, its secret key should not be derived by the proxy and the delegatee which is the community health service group, thus the IBPRE mechanism should achieve master secret secure. Its normal ciphertexts and re-encrypted ciphertexts should be also kept confidential for the adversaries including the cloud, the proxy etc, thus IBPRE should achieve IND-ID-CPA or IND-ID-CCA security.

4. Proposed Schemes and Security Analysis

4.1. New Identity Based Encryption

1. **Setup**$(\mathbf{1^k})$. Run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, \mathbb{G}_T, e)$. Next it generates g as generators of bilinear group of $\mathbb{G}$ with order p. For now, we assume public keys (ID) are elements in $\mathbb{Z}_p^*$. We also assume messages to be encrypted are elements in $\mathbb{G}_T$. Select random $t_1, t_2, t_3 \in \mathbb{Z}_p^*$, let $g_2 = g^{t_1}, g_3 = g^{t_3}, h = g^{t_2}$. Pick a random $\alpha \in \mathbb{Z}_p^*$, set $g_1 = g^\alpha$, that is,

$$\begin{aligned} &params = (g, g_1, g_2, g_3, h, p, \mathbb{G}, \mathbb{G}_T, e), \\ &msk = (\alpha, t_1, t_2, t_3) \end{aligned}$$

2. **KeyGen**$(\mathbf{msk}, \mathbf{params}, \mathbf{ID})$. Given $msk = (\alpha, t_1, t_2, t_3)$ and ID with $params$, the PKG picks random $x, y, n \in \mathbb{Z}_p^*$ and sets

$$\begin{aligned} d_{ID} \quad &= (d_1, d_2, d_3, d_4) \\ &= (\frac{\alpha + x}{\alpha ID + t_2} + y \bmod p, \quad g^x (g_1^{ID} h)^y, \quad g_3^x (g_1^{ID} h)^{-n}, \quad g_3^y g^n) \end{aligned}$$

3. **Encrypt**($\mathbf{ID}, \mathbf{params}, \mathbf{M}$). To encrypt a message $M \in \mathbb{G}_T$ under the public key $ID \in \mathbb{Z}_p^*$, pick a random $r \in \mathbb{Z}_p^*$ and compute

$$C_{ID} = (C_1, C_2, C_3, C_4) = (g^r, (g_2 g_3)^r, (g_1^{ID} h)^r, M e(g_1, g_2)^r)$$

4. **Decrypt**($\mathbf{sk_{ID}}, \mathbf{params}, \mathbf{C_{ID}}$). Given ciphertext $C_{ID} = (C_1, C_2, C_3, C_4)$ and the secret key $d_{ID} = (d_1, d_2, d_3)$ with *params*, compute

$$M = \frac{C_4 e(C_2, d_2)}{e(g_2, C_3^{d_1}) e(C_1, d_3) e(C_3, d_4)}$$

Correctness:

$$\begin{aligned} M' &= \frac{C_4 e(C_2, d_2)}{e(g_2, C_3^{d_1}) e(C_1, d_3) e(C_3, d_4)} \\ &= \frac{M e(g_1, g_2)^r e((g_2 g_3)^r, g^x (g_1^{ID} h)^y)}{e(g_2, ((g_1^{ID} h)^r)^{(\frac{\alpha+x}{\alpha ID + t_2} + y)}) e(g^r, g^{t_3 x} (g_1^{ID} h)^{-n})} \cdot \frac{1}{e((g_1^{ID} h)^r, g^{t_3 y} g^n)} \end{aligned}$$

$$\begin{aligned} &= \frac{M e(g_1, g_2)^r e((g_2 g_3)^r, g^x (g_1^{ID} h)^y)}{e(g_2, ((g_1^{ID} h)^r)^y) e(g_2, g^{xr}) e(g_2, g_1^r) e(g_3^r, g^x (g_1^{ID} h)^y)} \\ &= \frac{M e(g_1, g_2)^r e(g_2, (g^x (g_1^{ID} h)^y)^r)}{e(g_2, ((g_1^{ID} h)^r)^y) e(g_2, g^{xr}) e(g_2, g_1^r)} \\ &= \frac{M e(g_1, g_2)^r e(g_2, ((g_1^{ID} h)^y)^r)}{e(g_2, ((g_1^{ID} h)^r)^y) e(g_2, g_1^r)} \\ &= \frac{M e(g_1, g_2)^r}{e(g_2, g_1^r)} = M \end{aligned}$$

Here we compare our IBE scheme with some other existing IBE schemes, the results can be seen in Table 1. From this table we can see that our scheme is the most efficient for the re-encryption process, furthermore the security proof of our scheme is novel compared with the famous BF, BB1 and BB2 IBE. Our scheme can simulate the private key generation without knowing the master key α, as we rely on a denominator/numerator form technique to simulate the secret key generation, the concrete techniques can be seen in the below subsection. Furthermore, although our scheme can only be proved IND-CPA secure, it can be easily extended to be CCA-secure by using known techniques. We emphasise here that IND-CPA security in some cases is enough for E-health systems, for these systems are often organized in a closed environment and thus the users of them are often semi-trusted or trusted.

4.2. Security Analysis for IBE

Theorem 1. *Suppose the EXDBDH1 assumption holds in* $(\mathbb{G}, \mathbb{G}_T, e)$*, then our proposed* IBE *is* IND-sID-CPA *secure.*

Table 1: Feature Comparison

Scheme	W.R.O.	Efficient for re-encryption	Security proof technique
BF [8]	No	No	Random Oracle Model
BB1 [9]	Yes	No	Simulating without g^{α}
BB2 [9]	Yes	No	Simulating without g^{α}
Ours	Yes	Yes	Simulating without α

PROOF. Suppose $\mathcal{A}$ can attack our scheme, we construct an algorithm $\mathcal{B}$ solves the EXDBDH problem in $(\mathbb{G}, \mathbb{G}_T, e)$. On input $(g, g^a, g^b, g^c, g^{(b+c)d}, g^d, T)$, algorithm $\mathcal{B}$'s goal is to output 1 if $T = e(g,g)^{abd}$ and 0 otherwise. Let $g_1 = g^a, g_2 = g^b, g_3 = g^c$, that is, $t_1 = a, t_2 = b, t_3 = c$. Algorithm $\mathcal{B}$ works by interacting with $\mathcal{A}$ in a selective identity game as follows:

Initialization. The selective identity game begins with $\mathcal{A}$ first outputting an identity ID^* that it intends to attack.

Setup. To generate the system's parameters, algorithm $\mathcal{B}$ picks $\alpha' \in \mathbb{Z}_p^*$ at random and defines $h = g_1^{-ID^*} g^{\alpha'} \in \mathbb{G}$. It gives $\mathcal{A}$ the parameters $params = (g, g_1, g_2, g_3, h)$. Note that the corresponding master key, which is unknown to $\mathcal{B}$, is a.

Phase 1. $\mathcal{A}$ issues up to private key query on ID. $\mathcal{B}$ returns

$$\begin{aligned}
d_1^{sim} &= \frac{1}{(ID - ID^*)} + y \bmod p \\
&= \frac{a + x}{aID - aID^* + \alpha'} + y \bmod p \\
&= \frac{a + x}{aID + t_2} + y \bmod p \\
d_2^{sim} &= (g)^{(\frac{\alpha'}{ID - ID^*})} (g^a)^{y(ID - ID^*)} (g)^y \\
&= g^x (g^{a(ID-ID^*)} g)^y = g^x (g_1^{ID} h)^y \\
d_3^{sim} &= (g^c)^{(\frac{\alpha'}{ID - ID^*})} ((g^a)^{ID - ID^*} g^{\alpha'})^{-n} \\
&= g^{cx} (g_1^{ID} h)^{-n} = g_3^x (g_1^{ID} h)^{-n} \\
d_4^{sim} &= (g^c)^y g^n = g_3^y g^n
\end{aligned}$$

where $x = \frac{\alpha'}{ID - ID^*} \bmod p$ and y, n randomly chosen from $\mathbb{Z}_p^*$. We can verify $(d_1^{sim}, \cdots, d_4^{sim})$ is a valid private key for ID.

Challenge. When $\mathcal{A}$ decides that Phase 1 is over, it outputs two messages $M_0, M_1 \in \mathbb{G}$. Algorithm $\mathcal{B}$ picks a random bit b and responds with the ciphertext $C = (g^d, g^{(b+c)d}, (g^{\alpha\prime})^d, M_b \cdot T)$. Hence if $T = e(g,g)^{abd}$, then C is a valid encryption of M_b under ID^*. Otherwise, C is independent of b in the adversary's view.

Phase 2. $\mathcal{A}$ issues private key query on ID_i as he does in Phase 1 except $ID_i = ID^*$.

Guess. Finally, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. Algorithm $\mathcal{B}$ concludes its own game by outputting a guess as follows. If $b = b'$, then $\mathcal{B}$ outputs 1 meaning $T = e(g,g)^{abd}$. Otherwise it outputs 0 meaning $T \neq e(g,g)^{abd}$.

When $T = e(g,g)^{abd}$ then $\mathcal{A}$'s advantage for breaking the scheme is the same as $\mathcal{B}$'s advantage for solving EXDBDH problem.

4.3. New Identity Based Proxy Re-encryption

1. **Setup**$(\mathbf{1^k})$. Run $\mathbb{G}(1^n)$ to obtain $(\mathbb{G}, \mathbb{G}_T, e)$ with $\mathbb{G}$. Next it generates g as generators of $\mathbb{G}$. It chooses a one time signature scheme $\mathcal{S}$ and an IND-CCA2 symmetric encryption SE. It also chooses three hash functions $G : \{0,1\}^* \to \mathbb{Z}_p^*$[2], $H_1 : \mathbb{S} \to \mathbb{G}$ where $\mathbb{S}$ is the one time signature scheme's public key svk's space, $H_2 : G_T \to \mathcal{K}$ where $\mathcal{K}$ is the SE's key space. We also assume messages to be encrypted are elements in $\mathbb{G}_T$. Select random α, t_1, t_2, t_3 and compute (g_1, g_2, g_3, h) as the same as those in our IBE scheme, select random $s, s' \in \mathbb{Z}_p$ and compute $A = g^s$, that is

$$\begin{aligned} &params = (g, g_1, g_2, g_3, h, A, p, \mathbb{G}, \mathbb{G}_T, e, H, H_1, H_2, G, \mathsf{SE}, \mathcal{S}), \\ &msk = (\alpha, s, s', t_1, t_2, t_3) \end{aligned}$$

2. **KeyGen**$(\mathbf{msk}, \mathbf{params}, \mathbf{ID})$. Given $msk = (\alpha, t_1, t_2, t_3)$ and ID with $params$, the PKG picks random $x, y, x', y', N, n, n', z \in \mathbb{Z}_p^*$, computes $u_{ID} = sG(ID)$ and outputs the private key sk_{ID} associated with ID

$$\begin{aligned} sk_{ID} &= (d^A_{ID}, d^B_{ID}, d^C_{ID}) \\ d^A_{ID} &= (d_1, d_2, d_3, d_4, d_5, d_6) \\ &= (\frac{\alpha + x}{\alpha ID + t_2} + y \bmod p, g^x (g_1^{ID} h)^y, \\ &\quad g_3^x (g_1^{ID} h)^{-N}, g_3^y g^N, A^y g^n, A^x (g_1^{ID} h)^{-n}) \\ d^B_{ID} &= (d'_1, d'_2, d'_3) \\ &= (\frac{t_2 + x'}{\alpha ID + t_2} + y' \bmod p, A^{y'} g^{n'}, A^{x'} (g_1^{ID} h)^{-n'} g^{s'}) \\ d^C_{ID} &= (d_7, d_8) \\ &= (g_2^\alpha (g_1^{ID} h)^{u_{ID}} g^{zG(ID)}, g^{zG(ID)} g^{s'G(ID)}) \end{aligned}$$

3. **Encrypt**$(\mathbf{ID}, \mathbf{params}, \mathbf{M})$. To encrypt a message $M \in \mathbb{G}_T$ under the public key $ID \in \mathbb{Z}_p^*$, pick a random $r \in \mathbb{Z}_p^*$, a one time signature instance with public/private keys (svk, ssk), compute

$$\begin{aligned} C_{ID} &= (C_1, C_2, C_3, C_4, C_5, C_6, C_7) \\ &= (g^r, (g_2 g_3)^r, (g_1^{ID} h)^r, \mathtt{SE.Enc}(H_2(e(g_1, g_2)^r), M), H_1(svk)^r, svk, \sigma) \end{aligned}$$

where $\sigma = \mathcal{S}.\mathtt{sig}(ssk, C_1, C_2, C_3, C_4, C_5, C_6)$.

[2] G maps the identity to $\mathbb{Z}_p^*$ which can be used to identify different IBE users.

4. **ReKeygen**($\mathbf{d_{ID}}, \mathbf{params}, \mathbf{ID'}$). Choose randomly $k_3 \in \mathbb{Z}_p^*$, generate the re-encryption key $rk_{ID \to ID'}$ as following

$$\begin{aligned}
rk_{ID\to ID'} &= (rk_1, rk_2, rk_3, rk_4) \\
rk_1 &= \frac{1}{k_3}(d_1 \cdot ID' + d_1') \bmod p \\
&= \frac{1}{k_3}(\frac{(\alpha ID' + xID' + t_2 + x')}{\alpha ID + t_2} + yID' + y') \bmod p \\
&= \frac{(\alpha ID' + t_2 + k_1)}{k_3(\alpha ID + t_2)} + k_2 \bmod p
\end{aligned}$$

$$\begin{aligned}
rk_2 &= A^{k_3 \cdot G(ID')} = g^{k_3 \cdot s \cdot G(ID')} = g^{k_3 u_{ID'}} \\
rk_3 &= (d_5^{ID'} d_2')^{G(ID')} = g^{(s\cdot(yID'+y')+(nID'+n'))\cdot G(ID')} \\
&= g^{s\cdot(yID'+y')\cdot G(ID')} g^{(nID'+n')G(ID')} \\
&= g^{k_2 k_3 u_{ID'}} g^{(nID'+n')G(ID')} \\
rk_4 &= (d_6^{ID'} d_3')^{G(ID')} \\
&= \frac{g^{s\cdot(xID'+x')\cdot G(ID')} g^{s'G(ID')}}{(g_1^{ID} h)^{(nID'+n')G(ID')}}
\end{aligned}$$

where

$$k_1 = xID' + x', \quad k_2 = \frac{yID' + y'}{k_3}$$

5. **Reencrypt**($\mathbf{rk_{ID\to ID'}}, \mathbf{params}, \mathbf{C_{ID}}, \mathbf{ID'}$). Given ciphertext $C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6, C_7)$, first check C_{ID}'s validity:

$$\mathcal{S}.\texttt{Verify}(C_6, C_7) = \texttt{Yes}, \quad e(g, C_5) = e(C_1, H_1(C_6))$$

if these conditions are not satisfied, then return $\perp$, else compute

$$\begin{aligned}
\widehat{C_{ID'}} &= (C_1', C_2', C_3', C_4', C_5', C_6', C_7')_{ID'} \\
&= (C_1, C_2, C_3, C_4, e(C_3^{rk_1}, rk_2), rk_3, rk_4)
\end{aligned}$$

6. **Decrypt$_2$**($\mathbf{sk_{ID}}, \mathbf{params}, \mathbf{C_{ID}}$). Given ciphertext $C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6, C_7)$ and the secret key $sk_{ID} = (d_{ID}^A, d_{ID}^B, d_{ID}^C)$ where $d_{ID}^A = (d_1, d_2, d_3)$ with $params$, first check C_{ID}'s validity:

$$\mathcal{S}.\texttt{Verify}(C_6, C_7) = \texttt{Yes}, e(g, C_5) = e(C_1, H_1(C_6))$$

if these conditions can not be satisfied, then return $\perp$, else compute

$$\begin{aligned}
K &= H_2(\frac{e(g_2, C_3^{d_1}) e(C_1, d_3) e(C_3, d_4)}{e(C_2, d_2)}), \\
M &= \texttt{SE.Dec}(K, C_4)
\end{aligned}$$

and finally check M's validity by using SE's IND-CCA2 property.

7. $\mathbf{Deccrypt_1}(\mathbf{sk_{ID}}, \mathbf{params}, \widehat{\mathbf{C_{ID}}})$. Given the re-encrypted ciphertext $\widehat{C_{ID}} = (C'_1, C'_2, C'_3, C'_4, C'_5, C'_6, C'_7)_{ID}$ with $d^C_{ID} = (d_7, d_8)$ with $params$, decrypt the re-encrypted ciphertext as

$$K = H_2(\frac{e(C'_3, C'_6)e(C'_1, C'_7)e(C'_1, d_7)}{C'_5 e(C'_2, d_8)}),$$
$$M = \mathtt{SE.Dec}(K, C'_3)$$

and finally check M's validity by using SE's IND-CCA2 property.

Correctness: Assume the re-encrypted ciphertext is $\widehat{C_{ID}} = (C'_1, C'_2, C'_3, C'_4, C'_5, C'_6, C'_7)_{ID}$, which results from re-encrypting from ID_x to ID by using $rk_{ID_x \to ID}$. We can verify the correctness of $\mathsf{Deccrypt_1}(\mathsf{sk_{ID}}, \mathsf{params}, \widehat{\mathsf{C_{ID}}})$ as following

$$\begin{aligned}
T &= \frac{e(C'_3, C'_6)e(C'_1, C'_7)e(C'_1, d_7)}{C'_5 e(C'_2, d_8)} \\
&= \frac{e(C'_3, rk_3)e(C'_1, rk_4)e(C'_1, d_7)}{C'_5 e(C'_2, d_8)} \\
&= \frac{e((g_1^{ID_x}h)^r, g^{u_{ID}k_2k_3} g^{(nID+n')G(ID)})}{e(g^{k_3 u_{ID}}, (g_1^{ID_x}h)^{r(\frac{\alpha ID + t_2 + k_1}{k_3(\alpha ID_x + t_2)} + k_2)})} \cdot \frac{e(g^r, \frac{g^{k_1 u_{ID} g^{s'G(ID')}}}{(g_1^{ID_x}h)^{(nID+n')G(ID)}}) e(g^r, g_2^\alpha (g_1^{ID}h)^{u_{ID}} g^{zG(ID)})}{e(g^r, (g^z g^{s'})^{G(ID)})} \\
&= \frac{e((g_1^{ID_x}h)^r, g^{u_{ID}k_2k_3} g^{(nID+n')G(ID)})}{e(g^r, (g_1^{ID_x}h)^{(nID+n')G(ID)})} \\
&\quad \cdot \frac{1}{e(g^{k_3 u_{ID}}, (g_1^{ID_x}h)^{r(\frac{\alpha ID + t_2 + k_1}{k_3(\alpha ID_x + t_2)} + k_2)})} \cdot \frac{e(g^r, g^{k_1 u_{ID}}) e(g^r, g^{s'G(ID)}) e(g^r, g_2^\alpha (g_1^{ID}h)^{u_{ID}} g^{zG(ID)})}{e(g^r, g^{zG(ID)}) e(g^r, g^{s'G(ID)})} \\
&= \frac{e((g_1^{ID_x}h)^r, g^{u_{ID}k_2k_3}) e(g^r, g^{k_1 u_{ID}})}{e(g^{k_3 u_{ID}}, (g_1^{ID_x}h)^{k_2 r}) e(g^{k_3 u_{ID}}, (g_1^{ID}h)^{\frac{r}{k_3}})} = e(g_2^\alpha, g^r) \frac{e(g_2^\alpha (g_1^{ID}h)^{u_{ID}}, g^r) e(g^{zG(ID)}, g^r)}{e(g^{k_3 u_{ID}}, g^{\frac{k_1 r}{k_3}}) e(g^r, g^{zG(ID)})} \\
K &= H_2(T), \quad M = SE.Dec(K, C'_3)
\end{aligned}$$

4.4. Security Analysis for IBPRE

Theorem 2. *Suppose the EXDBDH assumption holds in* $(\mathbb{G}, \mathbb{G}_T, e)$, SE *is* IND-CCA2 *secure and* $\mathcal{S}$ *is strongly unforgeable, then our* IBPRE *scheme is* IND-sID-CCA2 *secure for the second level ciphertext.*

Proof. Suppose $\mathcal{A}$ can attack our scheme, we construct an algorithm $\mathcal{B}$ (or simulator $\mathcal{B}$) solves the EXDBDH problem in $(\mathbb{G}, \mathbb{G}_T, e)$.

Before describing $\mathcal{B}$, we first define an event F_{OTS} and bound its probability to occur. Let $C^* = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, svk^*, \sigma^*)$ denote the challenge ciphertext given to $\mathcal{A}$ in the game. Let F_{OTS} be the event that, $\mathcal{A}$ issues a decryption query for a re-encryption query $C^* = (C_1, C_2, C_3, C_4, C_5, svk^*, \sigma)$ where $(C_1, C_2, C_3, C_4, C_5) = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*)$ but $\sigma \neq \sigma^*$ and $\mathcal{S}.\mathtt{Verify}(\sigma, svk^*, (C_1, C_2, C_3, C_4, C_5)) = \mathtt{Yes}$. In the "find" stage, $\mathcal{A}$

has simply no information on svk^* . Hence, the probability of a pre-challenge occurrence of F does not exceed $q_O \cdot \delta$ if q_O is the overall number of oracle queries and δ denotes the maximal probability (which by assumption does not exceed $1/p$) that any one-time verification key svk is output by $\mathcal{S}$. In the "guess" stage F_{OTS} clearly gives rise to an algorithm breaking the strong unforgeability of the one-time signature. Therefore, the probability $Pr[F_{OTS}] \leq \frac{q_O}{p} + Adv^{OTS}$[3] must be negligible by assumption.

On input $(g, g^a, g^b, g^c, g^{(b+c)d}, g^d, T)$, algorithm $\mathcal{B}$'s goal is to output 1 if $T = e(g,g)^{abd}$ and 0 otherwise. Let $g_1 = g^a, g_2 = g^b, g_3 = g^c$, that is, $t_1 = a, t_2 = b, t_3 = c$. It chooses a one time signature scheme $\mathcal{S}$ and an IND-CCA2 symmetric encryption SE. It also chooses H, H_1, H_2, G as in the scheme. $\mathcal{B}$ works by interacting with $\mathcal{A}$ in a selective identity game as follows:

Initialization.The selective identity game begins with $\mathcal{A}$ first outputting an identity ID^* that it intends to attack.

Setup. To generate the system's parameters, algorithm $\mathcal{B}$ picks $\alpha' \in \mathbb{Z}_p^*$ at random and defines $h = g_1^{-ID^*} g^{\alpha'} \in \mathbb{G}$. It also picks random $w, r, s' \in \mathbb{Z}_p^*$, defines $s = r - bw$ and $A = g^s = g^{r-bw} = \frac{g^r}{g_2^w}$. It gives $\mathcal{A}$ the parameters $params = (g, g_1, g_2, g_3, h, A, H, H_1, H_2, G, \mathsf{SE}, \mathcal{S})$. Note that the corresponding master key, which is unknown to $\mathcal{B}$, is a.

Phase 1.

[3] Adv^{OTS} denotes the probability of breaking strong unforgeability of the one-time signature.

1. $\mathcal{A}$ *issues private key query on* ID *to* $O_{extract}$. $\mathcal{B}$ returns

$$\begin{aligned}
d_1^{sim} &= \frac{1}{(ID-ID^*)} + y \bmod p \\
&= \frac{a+x}{aID - aID^* + \alpha'} + y \bmod p \\
&= \frac{a+x}{aID + t_2} + y \bmod p \\
d_2^{sim} &= (g)^{(\frac{\alpha'}{ID-ID^*})}(g^a)^{y(ID-ID^*)}(g)^y \\
&= g^x(g^{a(ID-ID^*)}g)^y = g^x(g_1^{ID}h)^y \\
d_3^{sim} &= (g^c)^{(\frac{\alpha'}{ID-ID^*})}((g^a)^{ID-ID^*}g^{\alpha'})^{-N} \\
&= g^{cx}(g_1^{ID}h)^{-N} = g_3^x(g_1^{ID}h)^{-N} \\
d_4^{sim} &= (g^c)^y g^N = g_3^y g^N \\
d_5^{sim} &= A^y g^n, \\
d_6^{sim} &= A^{\frac{\alpha'}{ID-ID^*}}g^{\alpha'})^{-n}((g^a)^{ID-ID^*}g^{\alpha'})^{-n} \\
&= A^x(g_1^{ID}h)^{-n} \\
d_1'^{sim} &= \frac{-ID^*}{(ID-ID^*)} + y' \bmod p \\
&= \frac{a(-ID^*) + \alpha' + aID + x'}{aID + \alpha' - aID^*} + y' \bmod p
\end{aligned}$$

$$\begin{aligned}
&d_2'^{sim} = A^{y'}g^{n'}, \\
&d_3'^{sim} = A^{\frac{(-ID^*)\alpha'}{ID-ID^*}-\alpha'}((g^a)^{ID-ID^*}g^{\alpha'})^{-n'}g^{s'} \\
&= A^{x'}(g_1^{ID}h)^{-n'}g^{s'} \\
&d_7^{sim} = (g^b)^{-\alpha' wG(ID)}((g^a)^{(ID-ID^*)}g^{\alpha'})^{rG(ID)}g^{z'G(ID)} \\
&= g_2^{-\alpha' wG(ID)}(g_1^{(ID-ID^*)}g^{\alpha'})^{rG(ID)}g^{z'G(ID)} \\
&= g_2^{a(ID-ID^*)wG(ID)}(g_1^{(ID-ID^*)}g^{\alpha'})^{(r-bw)G(ID)}g^{z'G(ID)} \\
&= g_2^a(g_1^{(ID-ID^*)}g^{\alpha'})^{(r-bw)G(ID)} \\
&\cdot g^{a(ID-ID^*)wG(ID)-a+z'G(ID)} \\
&= g_2^a(g_1^{ID}h)^{sG(ID)} \\
&\cdot g^{a(ID-ID^*)wG(ID)-a+z'G(ID)} \\
&= g_2^a(g_1^{ID}h)^{sG(ID)}g^{zG(ID)} \\
&d_8^{sim} = (g^a)^{((ID-ID^*)wG(ID)-1)}g^{z'G(ID)}g^{s'G(ID)} \\
&= g^{a(ID-ID^*)wG(ID)-a+z'G(ID)}g^{s'G(ID)} \\
&= g^{zG(ID)}g^{s'G(ID)}
\end{aligned}$$

where $x = \frac{\alpha'}{ID-ID^*} \bmod p, x' = \frac{(-ID^*)\alpha'}{ID-ID^*} - \alpha' \bmod p,\ y, y', N, n, n', z'$ randomly

chosen from $\mathbb{Z}_p^*$, and $z = a(ID - ID^*)w - \frac{a}{G(ID)} + z'$ holds. We can verify $(d_1^{sim}, d_2^{sim}, \cdots, d_8^{sim})$ is a valid private key for ID. We call this simulation as "Normal Simulation".

2. *$\mathcal{A}$ issues rekey generation queries on (ID, ID') to re-encryption key extract oracle $O_{rkextract}$.*
   (a) $ID \neq ID^*$, in this case, ID' can be any identity. The simulator $\mathcal{B}$ first simulates $\mathsf{KeyGen}(msk, params, ID)$ as above and gets sk_{ID}. Then it runs $\mathsf{ReKeygen}(sk_{ID}$, $params, ID')$, and returns the result $rk_{ID \to ID'}$ to the adversary.
   (b) $ID = ID^*$, in this case, ID' can not be a corrupted identity. The simulator $\mathcal{B}$ uses some other technique to generate the re-encryption key. The simulator can generate the valid re-encryption key as following

$$
\begin{aligned}
d_1^{sim} &= \frac{k}{\alpha'} + y \bmod pn \\
&= \frac{a + k - a}{aID^* + \alpha' - aID^*} + y \bmod p \\
d_2^{sim} &= \frac{g^k}{(g^a)} g^{\alpha' y} \\
&= g^{k-a}(g^{\alpha'})^y = g^x (g_1^{ID^*} h)^y \\
d_3^{sim} &= \frac{(g^c)^k}{g^{ac}} (g^c)^{\alpha' y} = g^{c(k-a)} (g^c)^{\alpha' y} \\
&= g^{t_3(k-a)} (g^{\alpha'})^{t_3 y} = g^{t_3 x} (g_1^{ID^*} h)^{t_3 y} \\
d_4^{sim} &= A^y g^n, \\
d_5^{sim} &= A^{k-a} (g_1^{ID^* - ID^*} g^{\alpha'})^{-n} \\
&= A^x (g_1^{ID^* - ID^*} g^{\alpha'})^{-n} \\
d_1'^{sim} &= \frac{\alpha' + k'}{\alpha'} + y' \bmod p \\
&= \frac{a(-ID^*) + \alpha' + aID^* + k'}{aID^* + \alpha' - aID^*} \\
&\quad + y' \bmod p \\
d_2'^{sim} &= A^{y'} g^{n'} \\
d_3'^{sim} &= A^{aID^* + k'} g^{m'} (g_2 g_3)^{s'} \\
&= A^{x'} g^{m'} (g_2 g_3)^{s'} \\
d_4'^{sim} &= (g_1^{ID^* - ID^*} g^{\alpha'})^{n'} g^{m'} = (g^{\alpha'})^{n'} g^{m'}
\end{aligned}
$$

$$
\begin{aligned}
d_7^{sim} &= (g^b)^{-\alpha' wG(ID^*)} \\
&\quad \cdot((g^a)^{(ID^*-ID^*)}g^{\alpha'})^{rG(ID^*)} \\
&\quad \cdot(g^b)^{z'G(ID^*)}(g^{ac})^{((ID^*-ID^*)wG(ID^*)-1)} \\
&\quad \cdot(g^c)^{z'G(ID^*)} \\
&= g_2^a(g_1^{ID^*}h)^{sG(ID^*)} \\
&\quad (g_2g_3)^{-a+z'G(ID^*)} \\
&= g_2^a(g_1^{ID^*}h)^{sG(ID^*)}(g_2g_3)^{zG(ID^*)} \\
d_8^{sim} &= (g^a)^{((ID^*-ID^*)wG(ID^*)-1)} \\
&\quad \cdot g^{z'G(ID^*)} = g^{-a+z'G(ID^*)} \\
&= g^{zG(ID^*)}
\end{aligned}
$$

where $x = k - a, x' = aID^* + k'$, here $k, k', y, y', n, n', m, m', z'$ randomly chosen from $\mathbb{Z}_p^*$, and $z = -\frac{a}{G(ID^*)} + z'$ holds. After $\mathcal{B}$ generates private key for ID^*, it runs $\mathsf{ReKeygen}(sk_{ID^*}^{sim}, params,$ $ID')$ with $sk_{ID^*}^{sim}$, and returns the result $rk_{ID^* \to ID'}$ to the adversary. We call this simulation as "Special Simulation".

3. $\mathcal{A}$ *issues re-encryption queries on* $(C_{ID}, ID,$ $ID')$ *to re-encrypt oracle* $O_{reencrypt}$. $\mathcal{B}$ first runs $rk_{ID \to ID'} = \mathsf{ReKeygen}(sk_{ID}, params, ID')$, then runs $\mathsf{Reencrypt}(rk_{ID \to ID'}, C_{ID}, ID, ID')$ and returns the result to the adversary.
4. $\mathcal{A}$ *issues decryption queries on* $(\widehat{C_{ID'}}, ID')$ *to the first level ciphertext decrypt oracle* $O_{1decrypt}$ *under the only condition* $(\widehat{C_{ID'}}, ID') \neq \mathsf{Derivative}(C_{ID^*}^*, ID^*)$ *where* Derivative *defined in 2.4.*
   (a) $ID' \neq ID^*$, $\mathcal{B}$ first simulates $\mathsf{KeyGen}(msk,$ $params, ID')$ as in "Normal Simulation" 1, then runs $\mathsf{Decrypt}_1(sk_{ID'}, \widehat{C_{ID'}})$ and returns the result to the adversary.
   (b) $ID' = ID^*$, $\mathcal{B}$ first simulates $\mathsf{KeyGen}(msk,$ $params, ID^*)$ as in "Special Simulation" 2b, then runs $\mathsf{Decrypt}_1(sk_{ID^*}, \widehat{C_{ID^*}})$ and returns the result to the adversary.

Challenge. When $\mathcal{A}$ decides that Phase 1 is over, it outputs two messages $M_0, M_1 \in \mathbb{G}$, $\mathcal{B}$ picks a random bit b, a one time signature instance with public/private keys (svk, ssk), and responds with the ciphertext $C^* = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*,$ $C_6^*, C_7^*) = (g^d, g^{(b+c)d}, (g^{\alpha'})^d, \mathtt{SE.Enc}$ $(T, M_b), H_1(svk)^r, svk, \sigma)$ where $\sigma = \mathcal{S}(ssk, C_1^*,$ $C_2^*, C_3^*, C_4^*, C_5^*, C_6^*)$. Hence if $T = e(g,g)^{abd}$, then C^* is a valid encryption of M_b under ID^*. Otherwise, C^* is independent of b in the adversary's view.

Phase 2. $\mathcal{A}$ issues queries as he does in Phase 1 except natural constraints.

Guess. Finally, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. Algorithm $\mathcal{B}$ concludes its own game by outputting a guess as follows. If $b = b'$, then $\mathcal{B}$ outputs 1 meaning $T = e(g,g)^{abd}$. Otherwise it outputs 0 meaning $T \neq e(g,g)^{abd}$.

When $T = e(g,g)^{abd}$ then $\mathcal{A}$'s advantage is the same as $\mathcal{B}$'s advantage for solving EXDBDH problem. ∎

Theorem 3. *Suppose the EXDBDH assumption holds in* $(\mathbb{G}, \mathbb{G}_T, e)$ *and* SE *is* IND-CCA2 *secure, then our* IBPRE *scheme is* IND-sID-CCA2 *secure for the first level ciphertext.*

Proof. Following the same idea in the proof of theorem 2, we can prove this theorem, except this time the simulator needs to simulate re-encryption key on (ID^*, ID') where ID' is a corrupted identity. The simulator handles this query as following: it generates the private key for ID^* as in "Special Simulation" 2b. And runs $\mathsf{ReKeygen}(sk^{sim}_{ID^*}, params, ID')$ with $sk^{sim}_{ID^*}$, returns the result to the adversary. Now even if the adversary gets the simulated private key for ID' as in 1, it can not get any useful information from these keys because they are independent with $sk^{sim}_{ID^*}$, that is, $(x, x', y, y', n', n', z')_{ID'}$ for any ID' are independent with $(k, k', y, y', n, n', z')_{ID^*}$. ∎

We follow the way in [9] of using $H(ID)$[4] instead of ID to achieve full security for our IBPRE scheme.

Theorem 4. *In the standard model, let* $\mathcal{E}$ *be our* IBPRE *scheme, if it is a* (t, q_s, ϵ)*-selective identity secure* IBPRE *system (*IND-sID-CCA2*). Suppose* $\mathcal{E}$ *admits* N *distinct identities. Then* $\mathcal{E}$ *is also a* $(t, q_s, N\epsilon)$*-fully secure* IBPRE *(*IND-ID-CCA2*).*

Proof. The proof is directly following the proof for the similar theorem in [9], we omit it here due to space limitation. ∎

Theorem 5. *Suppose the EXDBDH assumption holds in* $(\mathbb{G}, \mathbb{G}_T, e)$*,* SE *is* IND-CCA2 *secure and* $\mathcal{S}$ *is strongly unforgeable, then our* IBPRE *scheme can achieve master secret security.*

Proof. As shown in [24], CCA2 security for the first level ciphertext implies the master secret security, thus our IBPRE scheme can achieve master secret security. ∎

Here we compare our IBPRE's scheme's security with other IBPRE schemes [17, 13, 31], In Table 2, we denote W/O Random Oracle as with/without random oracle. Note here Luo *et al.*'s IBPRE scheme is a generic construction, therefore their scheme can be in random oracle and standard model, and the underlying assumption can be various, but their generic construction is less efficient than our scheme. Also note that our IBPRE's security also rely on the underlying symmetric encryption scheme's IND-CCA2 security.

From the above table, we can conclude that our scheme is a new result on IBPRE. Our scheme can achieve master secret secure and is based on a novel IBE while all previous efficient IBPRE schemes are based on the traditional IBE.

[4]The space of $H(ID)$ is N.

Table 2: IBPRE Security Comparison

Scheme	Security	W/O Random Oracle	Assumption	Master Secret Secure	Underlying IBE
GA07A [17]	IND-ID-CPA	Random Oracle	DBDH	#	BF IBE
GA07B [17]	IND-ID-CCA	Random Oracle	DBDH	#	BF IBE
M07B [31]	IND-ID-CPA	Standard Model	DBDH	#	BB_1 IBE
CT07 [13]	IND-ID-CPA	Standard Model	DBDH	#	Waters' IBE
SXC08 [39]	IND-ID-CCA	Standard Model	DBDH	#	Waters' IBE
LZD+10 [29]	IND-ID-CCA	Standard Model	DBDH	!	Waters' IBE
WCW10 [45]	IND-ID-CCA	Random Oracle	DBDH	#	Variant of BF IBE
LHC10 [30]	IND-ID-CPA	Generic	Generic	!	Generic
Ours4.3	IND-ID-CCA	Standard Model	EXDBDH	!	New IBE

4.5. Security Analysis of Our E-health System

Here we briefly show that our schemes satisfy the security objectives of the E-health system.

1. For the patients, the physician group, and the community health service group, they use our proposed IBE to encrypt the EHRs, thus can achieve IND-ID-CPA or IND-ID-CCA security.
2. For the physician group which run the proxy re-encryption mechanism, his secret key can not be derived by the proxy and the delegatee, for our IBPRE scheme can achieve master secret security. His normal ciphertexts and re-encrypted ciphertexts can also achieve IND-ID-CPA or IND-ID-CCA security, for our IBPRE scheme has been proved IND-ID-CPA or IND-ID-CCA secure for the first level and the second level ciphertexts.

5. Performance Analysis

In this section, we give our performance analysis, basically we concentrate on the IBPRE's performance, for it is the critical part of our E-health system, especially, the re-encryption is the most used operation. Our IBE scheme are almost share the same efficiency with existing BB_1 or BB_2 IBE. We compared our IBPRE with other IBPRE schemes [17, 13, 31].

Notations: In Table 3, we denote Enc as encryption, Reenc as re-encryption, Dec as decryption, Ciph as ciphertext and Ciph-Len as ciphertext length, t_p, t_e and t_{me} represent the computational cost of a bilinear pairing, an exponentiation and a multi-exponentiation respectively. t_{se}, t_{sd} and t_{sv} represent the computational cost of once symmetric encryption, once symmetric decryption and once symmetric checking decryption results' validity. t_{s} and t_{v} represent the computational cost of a one-time signature signing and verification respectively. $|\mathbb{G}|$ and $|\mathbb{G}_T|$ denote the bit-length of an element in groups $\mathbb{G}$ and $\mathbb{G}_T$ respectively. Here $\mathbb{G}_e$ and $\mathbb{G}_T$ are the prime order bilinear groups. $|SE|$ denotes the bit length of once symmetric encryption. Finally, $|vk|$ and $|s|$ denote the bit length of the one-time signature's public key and a one-time signature respectively.

Note here our first level ciphertext maps second level ciphertext and second level ciphertext maps first level ciphertext in [17, 13]. Also note here GA07 and CT07 are

multi-hop IBPRE schemes but we just consider their single-hop variant. Here we omit the comparison between our IBPRE with SXC08 [39], LZD$^+$10 [29], WCW10 [45], LHC10 [30] schemes, for the following reasons: SXC08 [39], LZD$^+$10 [29] schemes are based on Waters' IBE, which make their schemes have large parameters; WCW10 [45] scheme can not achieve master secret secure and is only proved secure in the random oracle model; LHC10 [30] scheme is a generic construction.

Table 3: IBPRE Efficiency Comparison

Scheme	Enc	Check	Reenc	Dec		Ciph-Len	
				1stCiph	2ndCiph	1stCiph	2ndCiph
GA07B [17]	$1t_p + 1t_e$	$2t_p$	$2t_e + 2t_p$	$1t_e + 2t_p$	$2t_e + 2t_p$	$1\|G\| + 1\|G_e\|$ $+2\|m\| + \|id\|$	$1\|G\| + 1\|G_T\|$ $+1\|G_e\| + \|m\|$
LZD$^+$10 [29]	$5t_e$	$6t_p$	$6t_e$	$24t_p$	$8t_p$	$13\|G\| + 1\|G_T\|$	$4\|G\| + 1\|G_T\|$
WCW10 [45]	$5t_e$	$4t_p$	$2t_p$	$1t_e + 2t_p$	$1t_e + 4t_p$	$2\|G\| + 1\|G_T\|$ $+\|m\| + \|id\|$	$4\|G\| + 1\|G_T\|$ $\|id\| + \|m\|$
Ours 4.3	$2t_e + 2t_{me}$ $+1t_s + 1t_{se}$	$1t_v + 2t_p$	$t_e + t_p$	$2t_p + 1t_{sd}$	$5t_p + 1t_{sd}$ $+1t_{sv}$	$5\|G\| + 1\|G_T\|$ $+1\|SE\|$	$4\|G\| + 1\|s\|$ $+1\|vk\| + 1\|SE\|$

From the above table, we can conclude that our scheme seems to be a more directly construction of IBPRE for its re-encryption key is operated on the exponent instead of on the underlying group. Our scheme is particularly efficient for the cloud, especially for the IND-ID-CPA variant of our scheme. Compared with other IND-ID-CCA secure and master secret secure IBPRE schemes [17, 29], our scheme also has the high efficiency for the re-encryption process. Thus our scheme can greatly reduce the payment cost for the whole E-health cloud system users.

To further demonstrate our scheme's efficiency, we roughly evaluated its practical performance. We give the performance comparison results for GA07B, LZD+, WCW and Our schemes, according to the Benchmark of the famous JPBC library [4] based on TestBed 1 (Intel(R) Core(TM)2 Quad CPU Q6600 @2.4GHZ, 3GB Ram, Ubuntu 10.04). We have neglected some operations such as the computation cost of one-time symmetric encryption, one-time symmetric decryption and one-time checking for the decryption results' validity, one-time signature and verification. We choose type A pairings in JPBC and using the pairing preprocessing technique. We get the following computation cost comparison results from Figure 4,5,6,7,8, from which we can see our scheme is the most efficient scheme for checking and re-encryption process, while also remains among the most efficient ones for encryption, first level decryption and second level decryption. Note the cloud implements lots of re-encryption process for data sharing among users of E-health system, thus our scheme is the most efficient one for the cloud and can achieve cost-effective compared with other schemes.

6. Conclusion

In this paper, we have discussed how to integrate the IBE, IBPRE identity related techniques into a E-health cloud system to achieve its confidential property. We have

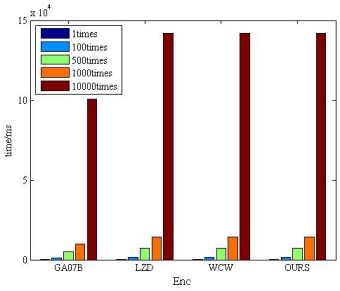

Figure 5: Encryption cost

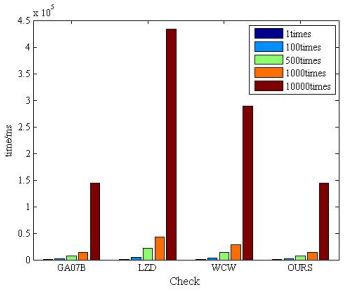

Figure 6: Checking cost

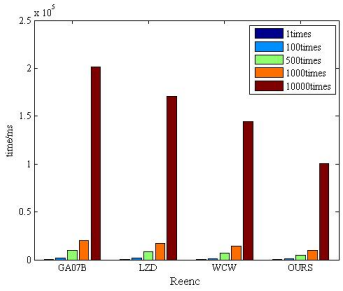

Figure 7: Re-encryption cost

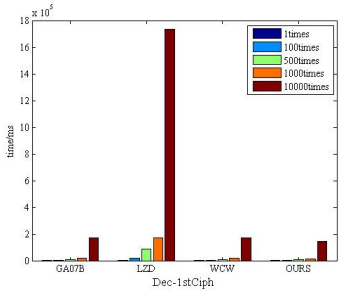

Figure 8: First level decryption cost

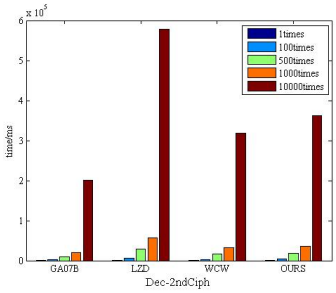

Figure 9: Second level decryption cost

presented the system model and show how to properly use these identity related primitives to achieve the security objective. We have also proposed a new IBE scheme, which does not rely in the IBE's three frameworks [11]. The main novelty is the way we have embedded the master key in the private key. We have proven this IBE is IND-sID-CPA secure in the standard model based on a related DBDH assumption in the bilinear groups. Based on this new IBE scheme, we have proposed a new IBPRE scheme, which is IND-ID-CCA2 secure, efficient for the proxy and master secret secure. Finally we have given the performance analysis on the critical part of our E-health system, the IBPRE scheme. These results showed the IBE, IBPRE identity related techniques are suitable for securing E-health cloud systems.

Acknowledgements

This work is extended from conference proceeding [47, 48]. This work is supported by Natural Science Foundation of Shaanxi Province (Grant No. 2014JM8300, 2014JQ8358, 2014JQ8307), the Changjiang Scholars and Innovation Research Team in University (Grant NO. IRT 1078), the Key Problem of NFSC-Guangdong Union Foundation (Grant NO. U1135002), the Major Nature Science Foundation of China (Grant NO. 61370078), China 863 project (Grant NO. 2015AA016007), the Fundamental Research Funds for the Center Universities (Grant NO. JY10000903001), Nature Science Foundation of China (Grant NO. 61103230, 61272492, 61202492, 61572390, 61370224). China 111 project (B08038).

References

[1] G. Ateniese, K. Fu, M. Green and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In *ACM NDSS 2005*, pages 29–43, 2005.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In *ACM Transactions on Information and System Security,* no. 1, pages 1–30. 2006.

[3] J. Aleman, I. Senor, P. Lozoya, A. Toval. Security and privacy in electronic health records: a systematic literature review. In *Journal of Biomedical Informatics 2013*, 24(1), pages 541-562, 2013.

[4] A. De Caro and V. Iovino. jPBC:java pairing based cryptography. In *Proceedings of the 16th IEEE Symposium on Computers and Communications*, ISCC, pages 850-855, 2011. http://gas.dia.unisa.it/projects/jpbc/.

[5] M. Barua, X. Liang, R. Lu and X. Shen. ESPAC: Enabling security and patient-centric access control for eHealth in cloud computing In *International Journal Security and Networks 2011*, 6(2/3), pages 67-76, 2011.

[6] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter. Patient controlled encryption: ensuring privacy of electronic medical records. Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW 09 , pages 103-114, 2009.

[7] M. Blaze, G. Bleumer and M. Strauss. Divertible protocols and atomic proxy cryptography. In *EUROCRYPT 1998*, volume 1403 of *LNCS*, pages 127–144, 1998.

[8] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229, 2001.

[9] D. Boneh and X.Boyen. Efficient selective-id secure identity based encryption without random oracles. In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238, 2004.

[10] D. Boneh and X.Boyen. Secure identity based encryption without random oracles. In *CRYPTO 2004*, volume 3152 of *LNCS*, pages 443–459, 2004.

[11] X. Boyen. A tapestry of identity-based encryption: practical frameworks compared, In *International Journal of Applied Cryptography*, Vol.1, No.1, pages 3–21, 2008.

[12] R. Canetti and S. Hohenberger. Chosen ciphertext secure proxy re-encryption. In *ACM CCS 2007*, pages 185–194, 2007. Full vision available at Cryptology ePrint Archive: http://eprint.iacr.org/2007/171.pdf.

[13] C. Chu and W. Tzeng. Identity-based proxy re-encryption without random oracles. In *ISC 2007*, volume 4779 of *LNCS*, pages 189–202, 2007.

[14] C. Chu, J. Weng, S.S.M. Chow, J. Zhou and R.H. Deng. Conditional proxy broadcast re-encryption. In *ACISP 2009*, volume 5594 of *LNCS*, pages 327–342, 2009.

[15] R. Deng, J. Weng, S. Liu and K. Chen. Chosen ciphertext secure proxy re-encryption without pairing. In *CANS 2008*, volume 5339 of *LNCS*, pages 1–17, 2008.

[16] Y. Dodis and A. Ivan. Proxy cryptography revisited. In Internet Society (ISOC): NDSS 2003, 2003.

[17] M. Green and G. Ateniese. Identity-based proxy re-encryption. In *ACNS 2007*, volume 4521 of *LNCS*, pages 288–306, 2007.

[18] C. Gentry. Practical identity-based encryption without random oracles. In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 445–464, 2006.

[19] L. Guo, C. Zhang, J. Sun, Y. Fang. PAAS: A Privacy-Preserving Attribute-based Authentication System for eHealth Networks. In *2012 32nd IEEE International Conference on Distributed Computing Systems, ICDCS 2012*, pages 224–233, 2012.

[20] J. Han, W. Susilo, Y. Mu. Identity-based data storage in cloud computing. In *Future Generation Computer Systems*, Vol 29(3), pp 673–681, 2013.

[21] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker. A type-and-identity-based proxy re-encryption scheme and its application in healthcare. In *SDM 2008*, volume 5159 of LNCS, pages 185–198, 2008.

[22] M. Jakobsson. On quorum controlled asymmetric proxy re-encryption. In *PKC 1999*, volume 1560 of *LNCS*, pages 112–121, 1999.

[23] Z. Khan, S. Sivakumar, W. Phillips, N. Aslam. A new patient monitoring framework and energy-aware peering routing protocol (EPR) for body area network communication. In *Journal of Ambient Intelligence and Humanized Computing*, Vol.5, pages 409-423, 2014.

[24] B. Libert and D. Vergnaud. Unidirectional chosen ciphertext secure proxy re-encryption. In *PKC 2008*, volume 4939 of *LNCS*, pages 360–379, 2008. full vision available at http://www.dice.ucl.ac.be/ libert/.

[25] M. Li, S. Yu, K. Ren, and W. Lou. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In: *SECURECOMM10*, pages 89-106, 2010.

[26] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. In: *IEEE transaction on parallel and distributed systems 2013*, 24(1), pages 131-143, 2013.

[27] J. Li, X. Chen, M. Li, J. Li, P. Lee, W. Lou. Secure deduplication with efficient and reliable convergent key management. In: *IEEE Transactions on Parallel and Distributed Systems*, 25(6), pages 1615-1625, 2014.

[28] J. Li, X. Huang, J. Li, X. Chen, Y. Xiang. Securely Outsourcing Attribute-based Encryption with Checkability. In: *IEEE Transactions on Parallel and Distributed Systems*, vol. 25 (8), pages 2201-2210, 2014.

[29] J. Lai, W. Zhu, R. Deng, S. Liu and W. Kou New constructions for identity-based unidirectional proxy re-encryption. In *Journal of Computer Science and Technology*, no. 25(4), pages 793–806. 2010.

[30] S. Luo, J. Hu and Z. Chen. New construction of identity-based proxy re-encryption. Cryptology ePrint Archive, Report 2010/444, 2010.

[31] T. Matsuo. Proxy re-encryption systems for identity-based encryption. In *PAIRING 2007*, volume 4575 of *LNCS*, pages 247–267, 2007.

[32] M. Naor. On cryptographic assumptions and challenges. In *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109, 2003.

[33] M. R. Ogiela, U. Ogiela. Linguistic extension for secret sharing (m, n)-threshold schemes. In *SecTech 2008 - 2008 International Conference on Security Technology, December 13-15, Hainan Island, Sanya, China*, ISBN: 978-0-7695-3486-2, DOI: 10.1109/SecTech.2008.15, pages 125–128, 2008,

[34] M. R. Ogiela, U. Ogiela. Security of linguistic threshold schemes in multimedia systems. In *Ernesto Damiani, Jechang Jeong, Robert J.Howlett,and Lakhmi C. Jain (Eds.): New Directions in Intelligent Interactive Multimedia Systems and Services - 2, Studies in Computational Intelligence (SCI)* vol. 226, Springer - Verlag Berlin Heidelberg, pages 13–20, 2009.

[35] M. Pirretti, P. Traynor, P. McDaniel and B. Waters. Secure attribute-based systems. In *Proceedings of ACM Symposium on Information, Computer and Communication Security*, pages 99–112, 2006.

[36] A. Sahai and B. Waters. Fuzzy identity-based encryption. In: *Proceedings of EUROCRYPT2005*, pages 457–473, 2005.

[37] J. Shao and Z. Cao. CCA-secure proxy re-encryption without pairing. In *PKC 2009*, volume 5443 of *LNCS*, pages 357–376, 2009.

[38] J. Shao, Z. Cao and P. Liu. SCCR: a generic approach to simultaneously achieve CCA security and collusion-resistance in proxy re-encryption. In *Security and Communication Networks*, Vol. 4(2), pages 122-135, 2011.

[39] J. Shao, D. Xing and Z. Cao. Identity-based proxy rencryption schemes with multiuse, unidirection and CCA security. Cryptology ePrint Archive: http://eprint.iacr.org/2008/103.pdf.

[40] R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive: http://eprint.iacr.org/2003/054.pdf.

[41] A. Shamir. Identity-based cryptosystems and signature Schemes. In *CRYPTO 1984*, volume 196 of *LNCS*, pages 47–53, 1984.

[42] Q. Tang, P. Hartel and W Jonker. Inter-domain identity-based proxy re-encryption. In *INSCRYPT 2008*, volume 5487 of *LNCS*, pages 332–347, 2008.

[43] Q. Tang. Type-based proxy re-encryption and its construction. In *INDOCRYPT 2008*, volume 5365 of *LNCS*, pages 130–144, 2008.

[44] B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127, 2005.

[45] H. Wang, Z. Cao, L. Wang. Multi-use and unidirectional identity-based proxy re-encryption schemes. In *Information Science*, No 180, pages 4042-4059, 2010.

[46] X. Wang and X. Yang On the insecurity of an identity based proxy re-encryption. In *Fundamental Informaticae*, no. 98(2-3), pages 277–281. 2010.

[47] X. Wang, W. Zhong. A new identity based encryption scheme. In *The International Conference on Biomedical Engineering and Computer Science*, IEEE Press, pages 381-384, 2010.

[48] X. Wang, W. Zhong. A new identity based proxy re-encryption scheme. In *The International Conference on Biomedical Engineering and Computer Science*, IEEE Press, pages 384-388, 2010.

[49] X. Wang, J. Ma, X. Yang. A new proxy re-encryption scheme for protecting critical information systems. In *Journal of Ambient Intelligence and Humanized Computing*, DOI: 10.1007/s12652-015-0261-3, 2015.

[50] J. Weng, R. H. Deng, C. Chu, X. Ding, and J. Lai. Conditional proxy re-encryption secure against chosen-ciphertext attack. In *ACM ASIACCS 2009*, Pages 322–332, 2009.

[51] M. Zhang, L. Wu, X. Wang, X. Yang. Unidirectional IBPRE scheme from lattice for cloud computation. In *Journal of Ambient Intelligence and Humanized Computing*, DOI: 10.1007/s12652-015-0260-4, 2015.